Amendments to the Specification:

Please replace paragraphs 12, 13, 16-23 and 25 in the specification with the corresponding numbered paragraphs as follows:

[12] Fig. 1[[A]] shows components in an Internet Protocol Rights Management (IPRM) system suitable for use with the present invention;

[13] Fig. [[1B]] 3 shows additional components relating to home domain access of information provided by a digital rights management (DRM) system such as the IPRM system of Fig. 1[[A]]; and

[16] Fig.1[[A]] shows components in an Internet Protocol Rights Management (IPRM) system suitable for use with the present invention.

[17] In Fig.1[[A]], logical components are shown in boxes with an indication of the physical component that is, preferably, used to perform the functionality of the logical component in parenthesis. Note that Fig.1[[A]] is merely a broad, general diagram of a one content distribution system. The functionality represented by logical components can vary from that shown in Fig.1[[A]] and still remain within the scope of the invention. Logical components can be added, modified or removed from those shown in Fig.1[[A]]. The physical components are examples of where logical components described in the diagram could be deployed. In general, aspects of the present invention can be used with any number and type of devices interconnected by a digital network.

[18] Fig.1[[A]] shows interfaces in the IPRM designed for secure content distribution and for the enforcement of rights of content and service providers. Such a system is used, for example, with satellite and cable television distribution channels where standard television content, along with digital information such as files, web pages, streaming media, etc., can be provided to an end user at home via a set-top box. IPRM system 100 is illustrated using a few exemplary logical components. In an actual system, there will be many more instances of specific logical components. For example, key management service 102 is intended to execute at a user, or viewer location. Naturally, there will be millions of viewers in a typical cable television network.

[19] The general purpose and operation of various of the entities of Fig.1[[A]], such as provisioning service (PS) 120, authentication service (AS) 112, entitlement service 124,

client processors and other servers and devices are well-known in the art. A system such as that shown in Fig.1[[A]] is discussed in more detail in co-pending patent application SYSTEM FOR DIGITAL RIGHTS MANAGEMENT USING DISTRIBUTED PROVISIONING AND AUHENTICATION, referenced above. The device security ratings system of the present invention can be used among any of the components and physical and logical devices shown in Fig.1[[A]] so that a decision can be made whether to transfer content, or other information, from an inquiring device to a target device.

[20] Fig. [[1B]] 3 shows additional components relating to home domain access of information provided by a DRM system such as the IPRM system of Fig.1[[A]]. The system of Fig. [[1B]] 3 can be considered as a subsystem, additional system, or overlay to that of Fig.1[[A]]. Although Fig. [[1B]] 3 shows hardware devices, such devices (e.g., viewer 158) can perform portions or combinations of the functions or services described in Fig.1[[A]].

[21] In Fig. [[1B]] 3, viewer 158 can be a display device, audio playback device, or other media presentation device, such as a television or computer. Viewer 158 is associated with local playback devices for playback of content, such as uncompressed digital media player 152, compressed digital media player 154 and analog media player 162. Such local devices are part of an "authorized domain" of equipment that is easily accessed by a user, or consumer, as illustrated by devices at 180. Note that the authorized domain can include additional networks, such as Ethernet, wireless, home phone network adapter (PNA), etc. and any number and types of devices for accessing, transferring, playing, creating, and managing content.

[22] The authorized domain presents a special problem to security since it typically places content directly at the control of a user. As indicated in Fig. [[1B]] 3, various devices may provide a user with content in various formats such as uncompressed, compressed, analog, stored, encrypted, etc. Other ways to provide content to the viewer are from remote devices such as conditional access center 150 using multicast streaming server 156 or unicast streaming server 160. Origin server 164 represents other content sources such as, e.g., a third party web site.

[23] Information can be stored locally or remotely from the authorized domain. Sensitive information such as content decryption keys 170, encrypted content 172 and

rules and metadata 174 might commonly be stored in devices that are accessible by the user. The system of the present invention can be used to improve security and rights enforcement in components and devices such as those shown in Fig. [[1B]] 3 by providing delivery of secure time signals to one or more of the components and devices. For example, a secure time service according to the present invention can be used to restrict playback of digital video as described in co-pending patent application entitled "ENFORCEMENT OF PLAYBACK COUNT IN SECURE HARDWARE FOR PRESENTATION OF DIGITAL PRODUCTIONS," referenced above.

[25] In Fig. 2, requesting device 202 (or "client") desires to obtain a secure time signal from secure time server 206 by using a ticket obtained from the Authentication Server 204 or from the Ticket Granting Service 218. The functionality in each of these components 202, 204, 206 and 218 can be implemented by any of the components and devices of Figs.1[[A]] and [[1B]] 3, or in any other suitable devices or components. Typically, Authentication Server 204 and Ticket Granting Service 218 are combined into a single server called KDC (Key Distribution Center).